



Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at <http://about.jstor.org/participate-jstor/individuals/early-journal-content>.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

XV. *On Systems of Linear Indeterminate Equations and Congruences.* By HENRY J. STEPHEN SMITH, *M.A., Fellow and Mathematical Lecturer of Balliol College, Oxford.*
Communicated by J. J. SYLVESTER, Esq., F.R.S.

Received January 17,—Read January 31, 1861.

THE theory of the solution, in positive or negative integral numbers, of systems of linear indeterminate equations, requires the consideration of rectangular matrices, the constituents of which are integral numbers. It will therefore be convenient to explain the meaning which we shall attach to certain phrases and symbols relating to such matrices.

A matrix containing p constituents in every horizontal row, and q in every vertical column, is a matrix of the type $q \times p$. We shall employ the symbol $\left\| \begin{smallmatrix} q \times p \\ A \end{smallmatrix} \right\|$, or (when it is not necessary that the type of the matrix should be indicated in its symbol) the simpler symbol $\|A\|$ to represent the matrix

$$\left\| \begin{array}{cccccc} A_{1,1}, & A_{1,2}, & \dots & A_{1,p} \\ A_{2,1}, & A_{2,2}, & \dots & A_{2,p} \\ \cdot & \cdot & \cdot & \cdot \\ A_{q,1}, & A_{q,2}, & \dots & A_{q,p} \end{array} \right\|$$

If $\|A\|$ and $\|B\|$ be two matrices of the same type, the equation $\|A\| = \|B\|$ indicates that the constituents of $\|A\|$ are respectively equal to the constituents of $\|B\|$; whereas the equation $|A| = |B|$ will merely express that the determinants of $\|A\|$ are equal to the corresponding determinants of $\|B\|$. The determinants of a matrix are, of course, the determinants of the greatest square matrices contained in it; similarly, its minor determinants of order i are the determinants of the square matrices of the type $i \times i$ that are contained in it. Matrices of the types $n \times (m+n)$ and $m \times (m+n)$ are said to be of complementary types; if $\|A\|$ and $\|B\|$ be two such matrices, we shall employ the equation

$$|A| = |B|$$

to express that each determinant of $\|A\|$ is equal to that determinant of $\|B\|$, by which it is multiplied in the development of the determinant of the square matrix $\left\| \begin{smallmatrix} A \\ B \end{smallmatrix} \right\|$. When

m and n are both uneven numbers, the signs of the determinants $\left| \begin{smallmatrix} A \\ B \end{smallmatrix} \right|$ and $\left| \begin{smallmatrix} B \\ A \end{smallmatrix} \right|$ are different: this occasions a certain ambiguity of sign in the interpretation of the equation $|A| = |B|$, which, however, will occasion no inconvenience. If $m = n$, the matrices $\|A\|$ and $\|B\|$ are at once of the same, and of complementary types; so that, in this case, the equation $|A| = |B|$ may stand for either of two very different sets of equations; but this

also is an imperfection of the notation here employed, which it is sufficient to have pointed out. If k denote any quantity whatever, it is hardly necessary to state that the equality

$$|A| = k \times |B|$$

implies that the determinants of $|A|$ are respectively k times the corresponding determinants of $|B|$.

Let $\|P\|$ be a square matrix of the type $n \times n$, and $\|Q\|$ a matrix of the type $n \times (n+m)$ (where $m \geq 0$), we shall understand by the matrix compounded of $\|P\|$ and $\|Q\|$, the matrix $\|X\|$ of the same type as $\|Q\|$, the constituents of which are defined by the equation

$$X_{i,j} = P_{i,1} Q_{1,j} + P_{i,2} Q_{2,j} + \dots + P_{i,n} Q_{n,j};$$

and we shall write

$$\|X\| = \|P\| \times \|Q\|;$$

in this equation $\|Q\|$ is said to be *premultiplied* by $\|P\|$, and $\|P\|$ to be *post-multiplied* by $\|Q\|$. This definition will suffice for our present purpose; as the only case of composition which we shall have to consider, is that in which the vertical dimensions of the matrices to be compounded are all equal, and in which every premultiplying matrix is square, so that if an oblong matrix present itself at all in a series of matrices to be compounded, it will occupy the last place in the series.

By the greatest divisor of a matrix we are to understand the greatest common divisor of the determinants of the matrix. If the matrix be square, its greatest divisor is, consequently, the determinant of the matrix. A *prime matrix* is one of which the greatest divisor is unity; *i. e.* the determinants of which are relatively prime. A prime square matrix (*i. e.* a matrix of which the determinant is unity) we shall call a *unit-matrix*.

In any system of linear equations, whether defective or redundant, or neither, we shall understand by the matrix of the system the matrix formed by the coefficients of the unknown quantities. If to this matrix we add an additional vertical column, composed of the absolute terms of the equations, the resulting matrix we shall term (for brevity) the *augmented* matrix of the system.

Lastly, when we have occasion to consider square matrices, the constituents of which, excepting those on the principal diameter, are zero, we shall represent them by symbols of the form

$$\|q_1, q_2, q_3, \dots, q_n\|,$$

where q_1, q_2, \dots, q_n are the constituents of the principal diameter.

Art. 2. If every determinant of the augmented matrix of a redundant system of linear equations is equal to zero, while the determinants of the unaugmented matrix are not all equal to zero, the system admits of one solution, and one only. And in particular if the matrix of the system be a prime matrix, the values of the unknown quantities which satisfy the system are integral numbers. For these values may be expressed as fractions having for their denominators any one of the determinants of the matrix; and these determinants are relatively prime.

Let $\|A\|$ be a given prime matrix of the type $n \times (n+m)$, $\|K\|$ a given matrix of the same type connected with $\|A\|$ by the equation

[illegible]

which implies that k is the greatest divisor of $\|\mathbf{K}\|$; then the symbolic equation

$$\|K\| = \|k\| \times \|A\|, \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (2.)$$

in which $\|k\|$ denotes a square matrix of the type $n \times n$, will admit of one solution, and one only.

For, to determine $k_{r,1}, k_{r,2}, \dots, k_{r,n}$, the constituents of the r th horizontal row of $\|k\|$, we have the redundant system

$$\left. \begin{array}{l} K_{r,i} = A_{1,i} k_{r,1} + A_{2,i} k_{r,2} + \dots + A_{n,i} k_{r,n} \\ i = 1, 2, 3, \dots, n+m \end{array} \right\} \dots \dots \dots (3.)$$

which is involved in the symbolic equation (2.). The matrix of this system is the prime matrix $\|A\|$; and the determinants of its augmented matrix are all equal to zero; for, by virtue of equation (1.), they are equal to the determinants

$$-\frac{1}{k} \times \begin{vmatrix} K_{r,1} & K_{r,2} & \dots & K_{r,n+m} \\ K_{1,1} & K_{1,2} & \dots & K_{1,n+m} \\ K_{2,1} & K_{2,2} & \dots & K_{2,n+m} \\ \cdot & \cdot & \cdot & \cdot \\ K_{n,1} & K_{n,2} & \dots & K_{n,n+m} \end{vmatrix}$$

in which two horizontal rows are identical. Thus the system (3.), and consequently the equation (2.), admits of one solution, and one only. It is evident that the determinant of $\|k\|$ is k . The case in which $m=0$ is not included in this demonstration; its proof, however, presents no difficulty, and may be omitted here.

A particular case of this theorem (that in which $n=2$) occurs in the ‘Disquisitiones Arithmeticae’ (see art. 234 of that work).

Art. 3. If every determinant of the augmented matrix of a redundant system of linear congruences be divisible by the modulus, while the greatest divisor of the unaugmented matrix is prime to the modulus, the system is resolvable and admits of only one solution. For if the modulus be represented by $P \times Q \times R \dots$, $P, Q, R \dots$ denoting powers of unequal primes, one (at least) of the determinants of the unaugmented matrix is prime to P , one (at least) is prime to Q , &c.; whence it may be inferred that the system is resolvable for each of the modules $P, Q, R \dots$, and admits of only one solution for each of them; it is therefore resolvable for their product $P \times Q \times R \dots$, and admits of only one solution for that modulus.

Let $\|K\|$ denote (as in the preceding article) a given matrix of the type $n \times (n+m)$, of which k is the greatest divisor; and let it be required to find the complete solution of the symbolic equation

[illegible]

in which $\|k\|$ is a square matrix of which the determinant is k , $\|A\|$ a prime matrix of

the same type as $\|K\|$, and in which the constituents of $\|A\|$ and $\|k\|$ are the unknown numbers.

We shall first obtain a particular solution of this equation, and then show how from any particular solution the complete solution may be deduced.

We may suppose that the constituents of any horizontal row of $\|K\|$ admit of no common divisor but unity; for if $\delta_1, \delta_2, \dots \delta_n$ be the greatest common divisors of the constituents of the horizontal rows of $\|K\|$, we find

$$\|K\| = \|\delta_1, \delta_2, \delta_3, \dots \delta_n\| \times \|K'\|, \quad \dots \dots \dots (5.)$$

$\|K'\|$ denoting a matrix the constituents of which are derived from those of $\|K\|$ by the relation

$$K'_{r,s} = \frac{1}{\delta_r} K_{r,s}; \quad \dots \dots \dots (6.)$$

so that the solution of equation (4.) depends on the solution of a similar equation for the matrix $\|K'\|$, in which the constituents of each horizontal row are relatively prime.

Let then the matrix $\left\| \begin{smallmatrix} r \times (n+m) \\ K \end{smallmatrix} \right\|$, *i. e.* the matrix

$$\left\| \begin{array}{cccc} K_{1,1}, K_{1,2}, \dots K_{1,n+m} \\ K_{2,1}, K_{2,2}, \dots K_{2,n+m} \\ \dots \dots \dots \dots \dots \dots \\ K_{r,1}, K_{r,2}, \dots K_{r,n+m} \end{array} \right\| \quad [1 \leq r \leq n],$$

be a prime matrix, but let the matrix $\left\| \begin{smallmatrix} (r+1) \times (n+m) \\ K \end{smallmatrix} \right\|$ admit of a greatest divisor μ .

Determine $\omega_1, \omega_2, \dots \omega_r$ by the system of congruences,

$$\left. \begin{array}{l} K_{1,i} \omega_1 + K_{2,i} \omega_2 + \dots K_{r,i} \omega_r \equiv K_{r+1,i} \pmod{\mu}, \\ i=1, 2, 3, \dots n+m \end{array} \right\} \quad \dots \dots \dots (7.)$$

(which, as we have just seen, is always resolvable), and in $\|K\|$ replace the constituents $K_{r+1,i}$ by the numbers

$$\frac{1}{\mu} [K_{r+1,i} - \sum_{s=1}^{s=r} \omega_s K_{s,i}];$$

we thus deduce from $\|K\|$ another matrix $\|K''\|$ connected with it by the relation $\|K\| = \mu \times \|K''\|$, and such that the matrix of its first $r+1$ horizontal rows is prime. By proceeding in this manner, we shall at last obtain a prime matrix $\|A_0\|$, which satisfies the equation $\|K\| = k \times \|A_0\|$; we may then, by the method of the last article, determine a square matrix $\|k_0\|$ satisfying the equation

$$\|K\| = \|k_0\| \times \|A_0\|, \quad \dots \dots \dots (8.)$$

and thus obtain a particular solution of the proposed equation (4.).

To deduce the general solution of that equation, let $\|k_1\|$ and $\|A_1\|$ be any two matrices satisfying it. We have therefore the equality

$$\|k_1\| \times \|A_1\| = \|k_0\| \times \|A_0\|, \quad \dots \dots \dots (9.)$$

If $\left\| \begin{smallmatrix} r \times (m+r) \\ a \end{smallmatrix} \right\|$ represent any matrix of the type $r \times (m+r)$, the determinants of which are not all equal to zero, and if $\lambda_1, \lambda_2, \dots \lambda_{m+r}$ be integers which satisfy the equations

$$\left. \begin{aligned} \sum_{k=1}^{k=m+r} a_{i,k} \lambda_k = 0, \\ i=1, 2, 3 \dots r \end{aligned} \right\} \dots \dots \dots (18.)$$

while $a_{r+1,1}, a_{r+1,2}, a_{r+1,3} \dots a_{r+1,m+r}$ are integers satisfying the inequality

$$\sum_{k=1}^{k=m+r} a_{r+1,k} \lambda_k \geq 0, \dots \dots \dots (19.)$$

the determinants of the matrix

$$\left\| \begin{smallmatrix} (r+1) \times (m+r) \\ a \end{smallmatrix} \right\|$$

are not all equal to zero.

For if $\sum_{k=1}^{k=m+r} a_{r+1,k} \lambda_k = 0$, it is evident that by combining this equation with the equations (18.), we may express each of the determinants $\theta \times \left\| \begin{smallmatrix} r \times (m+r) \\ a \end{smallmatrix} \right\|$ in succession as a linear function of the determinants of $\left\| \begin{smallmatrix} (r+1) \times (m+r) \\ a \end{smallmatrix} \right\|$. If, therefore, the former determinants do not all vanish, neither can the latter.

Let, then, $a_{m,1}, a_{m,2}, \dots a_{m,n+m}$ represent any particular solution (other, of course, than that in which every indeterminate is equal to zero) of the system (16.); and let $A_{n+1,1}, A_{n+1,2}, \dots A_{n+1,n+m}$ be integral numbers satisfying the inequality

$$\sum_{k=1}^{k=n+m} A_{n+1,k} a_{m,k} \geq 0; \dots \dots \dots (20.)$$

the system

$$\left. \begin{aligned} A_{i,1} x_1 + A_{i,2} x_2 + \dots + A_{i,n+m} x_{n+m} = 0 \\ i=1, 2, 3, \dots n+1 \end{aligned} \right\} \dots \dots \dots (21.)$$

(which is obtained by the addition of a single equation to the system (16.)) is itself an independent system, as appears from the principle just enunciated; its index of indeterminateness is therefore $m-1$. Let $\left\| \begin{smallmatrix} (m-1) \times (n+m) \\ a \end{smallmatrix} \right\|$ represent a complete set of independent solutions of (21.); it may then be inferred, from a second application of the same principle, that $\left\| \begin{smallmatrix} m \times (n+m) \\ a \end{smallmatrix} \right\|$ represents a complete set of independent solutions of the proposed system (16.). Thus the determination of a complete set of independent solutions of a system of which the index of indeterminateness is m , depends on the determination of a similar set of solutions for a system of which the index is lower by a unit. By successive reductions, therefore, we shall at last arrive at a system of which the index of indeterminateness is unity, the complete solution of which is of course immediately found by evaluating the determinants of its matrix.

The practical application of this method supposes only that we can always assign a *particular* solution of a system of the form (16.) or (21.). And this, it may be observed,

can always be done, either by trial, or by other obvious and not unsymmetrical expedients.

Art. 5. If $\|a\|$ represent the matrix of a complete set of independent solutions of the proposed system (16.), and $\|b\|$ be any matrix of the same type as $\|a\|$, and connected with $\|a\|$ by the equation

[illegible]

in which $\|k\|$ denotes a square matrix of which the determinant is not zero, it is evident that the constituents of $\|b\|$ are also a complete set of independent solutions. And, conversely, if $\|b\|$ be the matrix of a complete set of independent solutions, $\|a\|$ is also the matrix of a similar set. For if $\|K\|$ be the matrix composed of the first minors of $\|k\|$, so that

$$\|\mathbf{K}\| \times \|k\| = \|k, k, k, \dots\|,$$

we have from (22.),

$$\|K\| \times \|b\| = \|k, k, \dots, k, k\| \times \|a\|;$$

from which it appears that $\|k, k, \dots\| \times \|a\|$, and therefore $\|a\|$ itself, is the matrix of an independent set of solutions.

This observation enables us to obtain a complete set of relatively prime solutions, as soon as we have obtained an independent set. If $\|b\|$ be the matrix of the independent set, we have only to determine, by the method of art. 3, a square matrix $\|k\|$, and an oblong prime matrix $\|a\|$, satisfying the equation

$$\|b\| = \|k\| \times \|a\|;$$

the constituents of $\|a\|$ are then the terms of a set of fundamental solutions.

Or again, if in art. 4 we employ, instead of the inequality (19.), the equation

[illegible]

it is easily shown that if $\left\| \begin{smallmatrix} r \times (n+m) \\ a \end{smallmatrix} \right\|$ be a prime matrix, $\left\| \begin{smallmatrix} (r+1) \times (n+m) \\ a \end{smallmatrix} \right\|$ is also a prime matrix; so that, by following the method of that article, we may obtain directly a set of fundamental solutions of any proposed system. Only, it will be observed, that in this mode of obtaining such a set, we suppose that we can assign particular solutions, not only of systems of the form (16.), but also of equations of the form (23.).

Art. 6. The importance of fundamental sets of solutions in the theory of linear indeterminate equations is evident from the following proposition:—

“If $\|a\|$ represent a set of fundamental solutions of the system (16.), the complete solution of that system is contained in the formula

[illegible]

in which $\xi_1, \xi_2, \dots, \xi_m$ are absolutely indeterminate integral numbers."

For it is evident that every set of numbers included in (24.) satisfies (16.); and, conversely, if $a_{m+1, 1}, a_{m+1, 2}, \dots, a_{m+1, n+m}$ be any solution of (16.), the determinants of the

the relation in question is expressed by the formula

$$k \times |A| = K \times |a|, \quad (25.)$$

where it is to be remembered that the types of the matrices $\|A\|$ and $\|a\|$ are complementary; so that, as has been already observed (see art. 1), there is an ambiguity of sign in the equation (25.).

To obtain its demonstration, let Q and q denote the sums of the squares of the determinants of $\|A\|$ and $\|a\|$ respectively, and consider the determinant $\left| \frac{A}{a} \right|$. This determinant is certainly not zero, for multiplying it by itself, we find

$$\left| \frac{A}{a} \right|^2 = Q \times q. \quad (26.)$$

Let, then, $\left| \frac{A}{a} \right|$ be multiplied by any determinant of $\|A\|$; for example, by $\Sigma \pm A_{1,1}, A_{2,2}, \dots A_{n,n}$. Observing that $\Sigma \pm A_{1,1}, A_{2,2}, \dots A_{n,n}$ may assume the form

$$\begin{vmatrix} A_{1,1} & A_{2,1} & \dots & A_{n,1} & 0, 0, \dots, 0 \\ A_{1,2} & A_{2,2} & \dots & A_{n,2} & 0, 0, \dots, 0 \\ . & . & . & . & . \\ A_{1,n} & A_{2,n} & \dots & A_{n,n} & 0, 0, \dots, 0 \\ A_{1,n+1} & A_{2,n+1} & \dots & A_{n,n+1} & 1, 0, \dots, 0 \\ A_{1,n+2} & A_{2,n+2} & \dots & A_{n,n+2} & 0, 1, \dots, 0 \\ . & . & . & . & . \\ A_{1,n+m} & A_{2,n+m} & \dots & A_{n,n+m} & 0, 0, \dots, 1 \end{vmatrix}$$

we obtain the equation

$$\left| \frac{A}{a} \right| \times \Sigma \pm A_{1,1}, A_{2,2}, \dots A_{n,n} = Q \times \Sigma \pm a_{1,n+1}, a_{2,n+2}, \dots a_{m,n+m}, \quad . . . (27.)$$

in which we may permute the second set of indices in any manner consistent with the condition that $\left| \frac{A}{a} \right|$ should not change its sign; so that we may write

$$\left| \frac{A}{a} \right| \times |A| = Q \times |a|, \quad (28.)$$

the correspondence of the determinants in $|A|$ and $|a|$ being fixed by the matrix $\left\| \frac{A}{a} \right\|$. The equation (25.) is an immediate consequence of this result; and if in that equation we suppose the correspondence of the determinants to be still fixed by the matrix $\left\| \frac{A}{a} \right\|$, we shall have to write

$$k \times |A| = K \times |a|,$$

or

$$k \times |A| = -K \times |a|,$$

according as $\left| \frac{A}{a} \right|$ is a positive or negative number.

Then, if $\|u\|$ represent any unit-matrix of the type $n \times n$, and $\lambda_1, \lambda_2, \dots \lambda_n$ absolutely indeterminate integers, the complete solution of the problem is contained in the formula

$$\left. \begin{array}{l} \|u\| \times \|\gamma_{i,j} + \lambda_i C_j\| \\ i=1, 2, 3 \dots n \\ j=1, 2, 3 \dots n+1 \end{array} \right\} \dots \dots \dots (50.)$$

For if $\|x\|$ be any one of the matrices contained in that formula, it is readily seen that

$$\left| \begin{array}{c} C \\ x \end{array} \right| = \left| \begin{array}{c} C \\ \gamma \end{array} \right| = C_1 c_1 + C_2 c_2 + \dots + C_{n+1} c_{n+1} = 1.$$

Conversely, if $\|x\|$ be a matrix satisfying the equation $\left| \begin{array}{c} C \\ x \end{array} \right| = 1$, $\|x\|$ is included in the formula (50.). To show this, we observe that the complete solution of equation (48.) is contained in the formula

$$y_j = c_j + \sum_{i=1}^{i=n} \theta_{i,j} \lambda_i, j=1, 2, \dots n+1, \dots \dots \dots (51.)$$

in which $\|\theta\|$ is *any* set of fundamental solutions of the equation

$$C_1 y_1 + C_2 y_2 + \dots + C_{n+1} y_{n+1} = 0, \dots \dots \dots (52.)$$

and $\lambda_1, \lambda_2, \dots \lambda_n$ are indeterminate integers. The complete solution of the same equation (48.) is therefore supplied by the determinants of the matrix $\|\gamma_{i,j} + \lambda_i C_j\|$. For those determinants may be represented by the formula

$$c_j + \sum_{i=1}^{i=n} [i, j] \lambda_i, j=1, 2, 3, \dots n+1,$$

in which $[i, j]$ symbolizes a first minor of the determinant $\left| \begin{array}{c} C \\ \gamma \end{array} \right|$, so that

$$[i, j] = \frac{d \left| \begin{array}{c} C \\ \gamma \end{array} \right|}{d \gamma_{i,j}}.$$

But the numbers $[i, 1], [i, 2], \dots [i, n+1]$ satisfy (52.) for every value of i ; and, since $\left| \begin{array}{c} C \\ \gamma \end{array} \right| = 1$, the determinants of the matrix

$$\left\| \begin{array}{l} [i, j] \\ i=1, 2, 3, \dots n \\ j=1, 2, 3, \dots n+1 \end{array} \right\} \dots \dots \dots (53.)$$

are the numbers $C_1, C_2, \dots C_{n+1}$, and are therefore relatively prime. It follows from this that (53.) represents a set of fundamental solutions of (52.); *i. e.* that the complete solution of (48.) is represented by the determinants of $\|\gamma_{i,j} + \lambda_i C_j\|$. If then $\|x\|$ be a matrix satisfying the equation $\left| \begin{array}{c} C \\ x \end{array} \right| = 1$, since the determinants of $\|x\|$ evidently satisfy (48.), values can be assigned to $\lambda_1, \lambda_2, \dots \lambda_n$ which shall verify the equation

$$|\gamma_{i,j} + \lambda_i C_j| = |x|,$$

whence it follows that

$$\|x\| = \|u\| \times \|\gamma_{i,j} + \lambda_i C_j\|,$$

$\|u\|$ denoting a unit-matrix, *i. e.* $\|x\|$ is one of the matrices included in the formula (50.).

The result incidentally obtained in the foregoing analysis, that the complete solution

and

$$\left\| \begin{array}{cccccccc} 1, & 0, & 0, & \dots & 0 & , & 0 & , & \dots & 0 \\ 0, & 1, & 0, & \dots & 0 & , & 0 & , & \dots & 0 \\ 0, & 0, & 1, & \dots & 0 & , & 0 & , & \dots & 0 \\ . & . & . & . & . & . & . & . & . & . \\ 0, & 0, & 0, & \dots & u_{1,1}, & u_{1,2}, & \dots & u_{1,n} \\ 0, & 0, & 0, & \dots & u_{2,1}, & u_{2,2}, & \dots & u_{2,n} \\ . & . & . & . & . & . & . & . & . & . \\ 0, & 0, & 0, & \dots & u_{n,1}, & u_{n,2}, & \dots & u_{n,n} \end{array} \right\|$$

$\|\lambda\|$ denoting a matrix of the type $n \times m$ of which the constituents may be any numbers whatever, and $\|u\|$ a unit-matrix of the type $n \times n$. If for $\|\lambda\|$ we substitute the matrix

$$\|\mu\| = \|u\|^{-1} \times \|\lambda\|,$$

it is readily seen that we may invert the order of the factors in the expression of $\|v\|$; so that, using an abbreviated notation, the signification of which is evident, we may write either

$$\|v\| = \left\| \begin{array}{c} 1, 0 \\ \lambda, 1 \end{array} \right\| \times \left\| \begin{array}{c} 1, 0 \\ 0, u \end{array} \right\|,$$

or

$$\|v\| = \left\| \begin{array}{c} 1, 0 \\ 0, u \end{array} \right\| \times \left\| \begin{array}{c} 1, 0 \\ \mu, 1 \end{array} \right\|.$$

Substituting the latter expression of $\|v\|$ in the equation

$$\left\| \begin{array}{c} C \\ x \end{array} \right\| = \|v\| \times \left\| \begin{array}{c} C \\ \gamma \end{array} \right\|,$$

we immediately infer

$$\|x\| = \|u\| \times \|\gamma + \Sigma \mu C\|.$$

Every matrix satisfying the equation $\left\| \begin{array}{c} C \\ x \end{array} \right\| = 1$ is therefore comprised in the formula (55.); and since it is evident, conversely, that every matrix comprised in (55.) satisfies the equation, that formula contains the complete solution of the question.

A particular solution of the problem (which may be taken for $\|\gamma\|$) can be obtained as follows:—Complete the matrix $\|C\|$ by any n horizontal rows of constituents which do not cause the determinant of the resulting matrix to vanish. From this matrix a prime (*i. e.* a unit) matrix of the same type is to be deduced by the method of art. 3, a reduction which can always be effected without changing the prime matrix $\|C\|$.

Art. 11. The consideration of sets of fundamental solutions of linear systems is also of use in the theory of indeterminate systems containing terms not affected by any indeterminate. Let

$$\left. \begin{array}{l} A_{i,0} + A_{i,1}x_1 + A_{i,2}x_2 + \dots + A_{i,n+m} = 0 \\ i=1, 2, 3, \dots n \end{array} \right\} \dots \dots \dots (56.)$$

represent such a system; its general solution will assume the form

$$\left. \begin{array}{l} x_k = a_k + \sum_{\theta=1}^{\theta=m} \mu_{\theta} a_{k,\theta} \\ k=1, 2, 3, \dots n+m \end{array} \right\} \dots \dots \dots (57.)$$

where $\alpha_1, \alpha_2, \dots \alpha_{n+m}$ is a particular solution of (56.), $\mu_1, \mu_2, \dots \mu_m$ indeterminate numbers, and $\|\alpha\|$ a set of fundamental solutions of the system

$$\left. \begin{aligned} A_{i,1}x_1 + A_{i,2}x_2 + \dots + A_{i,n+m}x_{n+m} = 0 \\ i=1, 2, 3, \dots n \end{aligned} \right\} \quad (58.)$$

Whenever, therefore, the proposed system is resolvable, its complete solution involves m indeterminates; but in order that it should be resolvable, a certain condition must be satisfied by its coefficients. This condition is, "that the greatest divisors of its augmented and unaugmented matrices must be equal*." We shall call these divisors D and D_0 respectively, representing the matrices themselves by $\|A\|$ and $\|A_0\|$. That the condition is necessary may be seen by eliminating in turn every combination of $n-1$ indeterminates from (56). We thus find that every determinant of $\|A\|$ is divisible by D_0 , *i. e.* that D is divisible by D_0 ; but evidently D divides D_0 , so that $D_0=D$. To show that the condition is sufficient, as well as necessary, consider the system

$$\left. \begin{aligned} A_{i,0}x_0 + A_{i,1}x_1 + A_{i,2}x_2 + \dots + A_{i,n+m}x_{n+m} = 0 \\ i=1, 2, 3, \dots n \end{aligned} \right\}, \quad (59.)$$

and let $\left\| \begin{smallmatrix} (m+1) \times (n+m+1) \\ \theta \end{smallmatrix} \right\|$ represent a set of its fundamental solutions. To say that (56.) is resolvable, is the same thing as to say that (59.) admits of solutions in which the value of x_0 is unity; and (59.) will not, or will admit of such solutions according as $\theta_{1,0}, \theta_{2,0}, \dots \theta_{m,0}$ do, or do not admit of any common divisor beside unity. But, by the theorem of art. 7, those determinants of $\|\theta\|$ into which the column $\theta_{1,0}, \theta_{2,0}, \dots$ enters, are equal to the determinants of $\|A_0\|$, taken in a proper order and divided by D . If $D=D_0$, the determinants of $\|A_0\|$, divided by D , are relatively prime, and consequently those determinants of $\|\theta\|$ which contain $\theta_{1,0}, \theta_{2,0}, \dots \theta_{m,0}$ are also relatively prime; a conclusion which implies that $\theta_{1,0}, \theta_{2,0}, \dots \theta_{m,0}$ are themselves relatively prime, *i. e.* that the system (56.) is resolvable.

This criterion is not immediately applicable if the system (56.) be not independent, *i. e.* if the determinants of its augmented matrix $\|A\|$ be all equal to zero. But it may

* [This Theorem has already been given by M. IGNAZ HEGER (Memoirs of the Vienna Academy, vol. xiv. second part, p. 111). I regret that in the abstract of the present paper, which has been inserted in the 'Proceedings of the Royal Society,' no reference was made to M. HEGER's Memoir, with the contents of which I was unacquainted, at the time at which that abstract was prepared. M. HEGER's demonstration (adapted to the terminology here employed) is, in the main, as follows. (1) If the unaugmented matrix of an indeterminate system be prime, the system is always resolvable. For every determinate system, of which the matrix is a unit-matrix, is resolvable in integral numbers; and we may suppose the given indeterminate system to form part of such a determinate system (see art. 10, *suprà*). (2) The equation $\|A\| = \|D\| \times \|A'\|$, in which $\|D\|$ is a square matrix, having D for its determinant, and $\|A'\|$ a prime matrix of the same type as $\|A\|$, is always resolvable (see art. 3). We can therefore replace the given system (56.) by a system of which the augmented matrix is $\|A'\|$, and which is resolvable or irresolvable at the same time with the given system. But if $D_0=D$, the unaugmented matrix of this derived system is prime; *i. e.* if $D_0=D$, the proposed system is resolvable. (3) That the condition is necessary as well as sufficient may be proved as in the text.—Sept. 1861, H. J. S. S.]

be applied to any independent system, equivalent to the proposed system, and deduced linearly from it.

If we represent by D_k the greatest divisor of the matrix, deduced from the matrix of (59.) by omitting from it the column $A_{1,k}, A_{2,k}, \dots A_{n,k}$, we may enunciate the following proposition:—

“In every solution of the system (59.), the value of x_k is divisible by $\frac{D_k}{D}$; and, conversely, a solution of that system can always be assigned in which x_k shall have any given value divisible by $\frac{D_k}{D}$.”

It will be seen that the solution of (56.) depends, first, on the solution of (59.), and, secondly, on that of the indeterminate equation

$$\theta_{1,0}x_1 + \theta_{2,0}x_2 + \dots + \theta_{m+1,0}x_{m+1} = 1. \quad (60.)$$

If we represent the values of the indeterminates in this equation as the determinants of the matrix

$$\begin{matrix} & i=1, 2, 3, \dots m \\ \|\gamma_{i,j} + \mu_i \theta_{j,0}\| & \\ & j=1, 2, \dots m+1 \end{matrix}$$

(see art. 10), we may express the most general values of the indeterminates which satisfy (56.) in the determinantal form

$$x_k = \begin{vmatrix} & \theta_{1,k} & \theta_{2,k} & & \theta_{m+1,k} \\ \gamma_{1,1} + \mu_1 \theta_{1,0} & \gamma_{1,2} + \mu_1 \theta_{2,0} & \dots & \gamma_{1,m+1} + \mu_1 \theta_{m+1,0} \\ \gamma_{2,1} + \mu_2 \theta_{1,0} & \gamma_{2,2} + \mu_2 \theta_{2,0} & \dots & \gamma_{2,m+1} + \mu_2 \theta_{m+1,0} \\ \dots & \dots & \dots & \dots \\ \gamma_{m,1} + \mu_m \theta_{1,0} & \gamma_{m,2} + \mu_m \theta_{2,0} & \dots & \gamma_{m,m+1} + \mu_m \theta_{m+1,0} \end{vmatrix} \quad (61.)$$

Art. 12. We shall now indicate an important transformation of which any square matrix of integral numbers is susceptible. We begin with the following theorem:—

“If a given rectangular matrix be premultiplied by a unit matrix, the greatest common divisor of any vertical column of minor determinants is the same in the resulting as in the given matrix.”

For it is evident that any minor, either in the given or in the resulting matrix, is an integral and linear function of the minors formed from the same vertical columns in the other matrix.

Similarly, it may be shown that

“When a square matrix is post-multiplied by any prime rectangular matrix, the greatest common divisor of any horizontal row of minors is the same in the resulting rectangular matrix as in the given square matrix.”

For if

$$\left\| \begin{matrix} n \times (n+m) \\ A \end{matrix} \right\| = \left\| \begin{matrix} n \times n \\ B \end{matrix} \right\| \times \left\| \begin{matrix} n \times (n+m) \\ C \end{matrix} \right\|,$$

2 u 2

where $\|C\|$ is a prime matrix, it is clear that every minor of $\|A\|$ is a linear function of the minors formed from the same horizontal rows of $\|B\|$; so that if a and b be the greatest common divisors of any corresponding horizontal rows of minors in those two matrices, a is divisible by b . But again, if θ be any one of the determinants of $\|C\|$, and s be the order of the minors under consideration, any minor of $\|B\|$, after multiplication by θ^s , may be expressed as a linear function of a certain group of the minors taken from the same horizontal rows of $\|A\|$. Consequently $\theta^s \times b$ is divisible by a ; or, since θ may have any one of a series of values which are relatively prime, b is divisible by a , i. e. $b=a$.

By combining these results we obtain the theorem.

“If $\nabla_n, \nabla_{n-1}, \nabla_{n-2}, \dots \nabla_1$ represent the greatest common divisors of all the minors of order $n, n-1, \dots 1$, respectively which can be formed out of a given square matrix, these numbers will remain unchanged, when the given matrix is premultiplied by any unit-matrix, and post-multiplied by any prime matrix whatsoever.”

Art. 13. Let θ , the determinant of the square matrix $\begin{vmatrix} n \times n \\ a \end{vmatrix}$, be a positive number, different from zero. It may be shown that by post-multiplication with a properly assumed unit $\|a\|$, the matrix $\|a\|$ can be reduced to the form

$$\begin{vmatrix} \mu_1, r_{1,2}, r_{1,3} \dots r_{1,n} \\ 0, \mu_2, r_{2,3} \dots r_{2,n} \\ 0, 0, \mu_3 \dots r_{3,n} \\ \dots \dots \dots \dots \dots \dots \\ 0, 0, 0 \dots \mu_n \end{vmatrix}, \dots \dots \dots (62.)$$

where $\mu_1, \mu_2, \dots \mu_n$ are positive numbers, such that $\mu_1 \times \mu_2 \times \dots \times \mu_n = \theta$, and the constituents $r_{i,k}$ satisfy the inequalities

$$0 \leq r_{i,k} < \mu_i \dots \dots \dots (63.)$$

This was first observed by GAUSS for the case $n=2$; by SEEBER for $n=3$; and the general theorem has been enunciated by M. HERMITE*. Its precise statement is

“Every matrix of the type $n \times n$ is equivalent (by post-multiplication) to one, and only one, of the *reduced* matrices included in the formula (62.).”

To show this, let $v_{1,1}, v_{2,1}, \dots v_{n,1}$ be the integral and relatively prime numbers which satisfy the equations

$$\left. \begin{aligned} a_{i,1} v_{1,1} + a_{i,2} v_{2,1} + \dots a_{i,n} v_{n,1} &= 0 \\ i &= 2, 3, \dots n \end{aligned} \right\}, \dots \dots \dots (64.)$$

and the inequality

$$a_{1,1} v_{1,1} + a_{1,2} v_{2,1} + \dots a_{1,n} v_{n,1} > 0.$$

Then it is evident that, if $\|v\|$ be a unit-matrix of which $v_{1,1}, v_{2,1}, \dots v_{n,1}$ form the first column, the matrix $\|a\| \times \|v\|$ will assume the form

* GAUSS, Disq. Arith. art. 213; SEEBER, “Untersuchungen ueber die Eigenschaften der positiven ternären quadratischen Formen” (Mannheim, 1831), art. 31; M. HERMITE, CRELLE, vol. xli. p. 192.

$$\left\| \begin{array}{cccc} \mu_1, & b_{1,2}, & b_{1,3}, & \dots b_{1,n} \\ 0, & b_{2,2}, & b_{2,3}, & \dots b_{2,n} \\ 0, & b_{3,2}, & b_{3,3}, & \dots b_{3,n} \\ \cdot & \cdot & \cdot & \cdot \\ 0, & b_{n,2}, & b_{n,3}, & \dots b_{n,n} \end{array} \right\|, \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad (65.)$$

where $\mu_1 = a_{1,1}, v_{1,1} + a_{1,2}, v_{2,1} + \dots a_{1,n}, v_{n,1}$.

If this matrix be post-multiplied by the unit,

$$\left\| \begin{array}{cccc} 1, & k_2, & k_3, & \dots k_n \\ 0, & 1, & 0, & \dots 0 \\ 0, & 0, & 1, & \dots 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0, & 0, & 0, & \dots 1 \end{array} \right\|$$

the constituents $b_{1,i}$ will be changed into $b_{1,i} + \mu_1 k_i$, while all the other constituents will remain unaltered; so that by assigning proper values to the numbers $k_2 \dots k_n$, we may bring the given matrix $\|a\|$ into the form

$$\left\| \begin{array}{cccc} \mu_1, & r_{1,2}, & r_{1,3}, & \dots r_{1,n} \\ 0, & b_{2,2}, & b_{2,3}, & \dots b_{2,n} \\ 0, & b_{3,2}, & b_{3,3}, & \dots b_{3,n} \\ \cdot & \cdot & \cdot & \cdot \\ 0, & b_{n,2}, & b_{n,3}, & \dots b_{n,n} \end{array} \right\|$$

where $r_{1,i}$ verifies the inequality

$$0 \leq r_{1,i} < \mu_1.$$

From this it is easy to infer that if a matrix of the type $(n-1) \times (n-1)$ can be reduced to the form (62.), the same reduction is possible for a matrix of the type $n \times n$, i. e. since that reduction is possible when $n=1, n=2, \dots$ it is possible for every value of n .

To prove that $\|a\|$ is equivalent (by post-multiplication) to only one of the *reduced* matrices (62.), it is sufficient to show that no two reduced matrices can be equivalent. If $\|a\|$ and $\|a'\|$ be two reduced matrices, and $\|v\|$ a unit-matrix, such that $\|a\| \times \|v\| = \|a'\|$, it may be inferred, by comparing the corresponding constituents of the two matrices $\|a\| \times \|v\|$ and $\|a'\|$ (beginning with the lowest horizontal rows of each and proceeding upwards), that all the constituents of $\|v\|$ which lie below its principal diameter are zero; and consequently that the constituents of the principal diameter itself are all positive units. Further, that the constituents above the principal diameter of $\|v\|$ are likewise zero, may be established (for each line of constituents parallel to the diameter, beginning with that nearest to it) by means of the inequalities (63.) which are satisfied by the constituents both of $\|a\|$ and $\|a'\|$. It thus appears that two reduced matrices cannot be equivalent, without being identical. It will be observed that the reducing unit is unique;

i. e. that only one post-multiplying unit can be assigned by which a given matrix can be reduced to the form (62.).

If instead of reducing the given matrix $\|a\|$ by post-multiplication we employ a pre-multiplying unit, we obtain the following theorem:—

“Every matrix of the type $n \times n$ and of determinant θ is equivalent (by pre-multiplication) to one, and only one of the matrices included in the formula (62.), in which $\mu_1, \mu_2 \dots$ are positive, $\mu_1, \mu_2 \dots \mu_n = \theta$, and $r_{i,k}$ satisfies the inequality

$$0 \leq r_{i,k} < \mu_k. \quad \dots \dots \dots (66.)$$

Art. 14*. The transformation to which we have referred in art. 12 is obtained by employing simultaneously a pre-multiplying and a post-multiplying unit-matrix. It is expressed by the equation

$$\|a\| = \|a\| \times \left\| \frac{\nabla_n}{\nabla_{n-1}}, \frac{\nabla_{n-1}}{\nabla_{n-2}}, \dots \frac{\nabla_1}{\nabla_0} \right\| \times \|\beta\|, \quad \dots \dots \dots (67.)$$

in which $\|a\|$ is a given square matrix of the type $n \times n$, $\|a\|$ and $\|\beta\|$ are unit-matrices, and $\nabla_n, \nabla_{n-1}, \nabla_{n-2}, \dots \nabla_1, \nabla_0$ are the determinant and greatest common divisors of the minor determinants of $\|a\|$, so that, in particular, ∇_n is the determinant of $\|a\|$, ∇_{n-1} the greatest common divisor of its minor determinants of order $n-1$, ∇_1 the greatest common divisor of its constituents, and $\nabla_0 = 1$. The units $\|a\|$ and $\|\beta\|$ are not absolutely determined, but admit, when $n > 1$, of an infinite number of different values. If $n = 1$, it is evident that the formula (67.) is verified; for we have the identical equation $\|a\| = \|1\| \times \left\| \frac{\nabla_1}{\nabla_0} \right\| \times \|1\|$. It is therefore sufficient to show that, if the transformation indicated in the formula can be effected for matrices of the type $(n-1) \times (n-1)$, it can also be effected for matrices of the type $n \times n$. The demonstration depends on an elementary principle, which it is worth while to enunciate separately.

“If

$$\left. \begin{aligned} U_i &= A_{i,1}x_1 + A_{i,2}x_2 + \dots + A_{i,n+m}x_{n+m}, \\ i &= 1, 2, 3, \dots n \end{aligned} \right\} \dots \dots \dots (68.)$$

denote a system of n linear functions of $n+m$ indeterminates, ($m \geq 0$), and if the constituents of the matrix $\|A\|$ do not admit of any common divisor, it is always possible to assign integral values to $x_1, x_2, \dots x_{n+m}$, which shall render $U_1, U_2, \dots U_n$ relatively prime.”

For, in the first place, we can obtain values for $U_1, U_2, \dots U_n$, which shall not have any common divisor with a given number M . Let $p, q, r \dots$ be the different prime divisors of M ; one at least of the constituents of $\|A\|$, for example $A_{i,j}$, is prime to p . Attributing to x_j a value prime to p , and values divisible by p to the remaining indeterminates, we shall obtain for U_i a value which is certainly prime to p . Similarly, by subjecting the indeterminates to proper congruential conditions with respect to the modules q, r, \dots , we can render one, at least, of the functions U prime to q , one prime to r , and

* [This article has been in great part rewritten since the paper was read. The demonstration is not essentially changed, but is presented in what seems to be a simpler form.—Sept. 1861, H. J. S. S.]

so on; *i. e.* since we can assign to the indeterminates values simultaneously satisfying all these congruential conditions, we can give to $U_1, U_2, \dots U_n$ values the greatest common divisor of which is prime to M . Let D_n be the greatest divisor of $\|A\|$, D_{n-1} the greatest common divisor of the first minors of $\|A\|$; and let $C_1, C_2, \dots C_n$ be a set of simultaneous values of $U_1, U_2, \dots U_n$, having a greatest common divisor c , which is prime to $\frac{D_n}{D_{n-1}}$. Since the equations

$$\begin{aligned} A_{i,1}x_1 + A_{i,2}x_2 + \dots + A_{i,n+m}x_{n+m} &= C_i, \\ i &= 1, 2, 3, \dots n \end{aligned}$$

are resolvable, it will follow from the condition of resolvability (see art. 11), that the determinants of its augmented matrix, and in particular those which contain the column $C_1, C_2, \dots C_n$, are divisible by D_n . Let $\theta \times c \times D_{n-1}$ be the greatest common divisor of these last determinants; then $\theta \times c \times D_{n-1}$ is divisible by D_n , *i. e.* θ is divisible by $\frac{D_n}{D_{n-1}}$. It appears from this, that the condition of resolvability is satisfied by the system

$$\begin{aligned} A_{i,1}x_1 + A_{i,2}x_2 + \dots + A_{i,n+m}x_{n+m} &= \frac{C_i}{c}, \\ i &= 1, 2, 3, \dots n, \end{aligned}$$

that is to say, it is possible to obtain a simultaneous system of relatively prime values for $U_1, U_2, \dots U_n$.

To apply this principle to the transformation of the matrix $\|a\|$, let

$$[a_{i,j}] = \frac{1}{\nabla_{n-1}} \frac{d\nabla_n}{da_{i,j}}. \quad \dots \dots \dots (69.)$$

The constituents of the matrix $\| [a] \|$ do not admit of any common divisor; consequently, in the system

$$\left. \begin{aligned} [a_{i,1}]b_{1,1} + [a_{i,2}]b_{2,1} + \dots + [a_{i,n}]b_{n,1} &= u_{i,1}, \\ i &= 1, 2, 3, \dots n \end{aligned} \right\}, \quad \dots \dots \dots (70.)$$

we can assign values to $b_{1,1}, b_{2,1}, \dots b_{n,1}$, which shall render $u_{1,1}, u_{2,1}, \dots u_{n,1}$ relatively prime. Let $\|u\|$ denote a unit-matrix of which the first column is $u_{1,1}, u_{2,1}, \dots u_{n,1}$; and $\|b\|$ a square matrix of which the first column is $b_{1,1}, b_{2,1}, \dots b_{n,1}$, and of which the remaining constituents are defined by the equations

$$\left. \begin{aligned} b_{i,j} &= a_{i,1}u_{1,j} + a_{i,2}u_{2,j} + \dots + a_{i,n}u_{n,j} \\ i &= 1, 2, 3, \dots n \\ j &= 2, 3, \dots n. \end{aligned} \right\} \quad \dots \dots \dots (71.)$$

Observing that the systems (69.) and (70.) involve the inverse system,

$$\left. \begin{aligned} a_{i,1}u_{1,1} + a_{i,2}u_{2,1} + \dots + a_{i,n}u_{n,1} &= \frac{\nabla_n}{\nabla_{n-1}} b_{i,1}, \\ i &= 1, 2, 3, \dots n, \end{aligned} \right\} \quad \dots \dots \dots (72.)$$

we infer that the matrices $\|u\|$ and $\|b\|$ verify the equation

$$\|a\| \times \|u\| = \|b\| \times \left\| \frac{\nabla_n}{\nabla_{n-1}}, 1, 1, \dots \right\|, \quad \dots \dots \dots (73.)$$

in which $\left\| \frac{\nabla_n}{\nabla_{n-1}}, 1, 1, \dots \right\|$ denotes a matrix of the type $n \times n$. It follows from (73.) that ∇_{n-1} is the determinant of $\|b\|$; let that matrix be reduced by premultiplication with a unit-matrix; and let

$$\|b\| = \|v\| \times \|\nabla_{n-1}\|, \quad \dots \quad (74.)$$

where $\|v\|$ is the reducing unit, and $\|\nabla_{n-1}\|$ the reduced matrix,

$$\left\| \begin{array}{cccc} \mu_1, & r_{1,2}, & r_{1,3} & \dots r_{1,n} \\ 0, & \mu_2, & r_{2,3} & \dots r_{2,n} \\ 0, & 0, & \mu_3 & \dots r_{3,n} \\ \dots & \dots & \dots & \dots \\ 0, & 0, & 0 & \dots \mu_n \end{array} \right\|, \quad \dots \quad (75.)$$

so that (73.) assumes the form

$$\|a\| = \|v\| \times \|\nabla_{n-1}\| \times \left\| \frac{\nabla_n}{\nabla_{n-1}}, 1, 1, \dots \right\| \times \|u\|^{-1}. \quad \dots \quad (76.)$$

It may be proved that in (75.) $\mu_1=1, r_{1,2}=0, r_{1,3}=0 \dots r_{1,n}=0$. For since the matrix $\|\nabla_{n-1}\| \times \left\| \frac{\nabla_n}{\nabla_{n-1}}, 1, 1, \dots \right\|$ is derived from $\|a\|$ by multiplication with unit-matrices, ∇_{n-1} is the greatest common divisor of the first minors of $\|\nabla_{n-1}\| \times \left\| \frac{\nabla_n}{\nabla_{n-1}}, 1, 1, \dots \right\|$. Therefore ∇_{n-1} divides $\mu_2 \times \mu_3 \times \dots \times \mu_n$, which is one of those minors; but also $\nabla_{n-1} = \mu_1 \times \mu_2 \dots \times \mu_n$; *i. e.* $\mu_1=1, \mu_2 \times \mu_3 \times \dots \times \mu_n = \nabla_{n-1}$, and the product $\|\nabla_{n-1}\| \times \left\| \frac{\nabla_n}{\nabla_{n-1}}, 1, 1, \dots \right\|$ assumes the form

$$\left\| \begin{array}{cccc} \frac{\nabla_n}{\nabla_{n-1}}, & r_{1,2}, & r_{1,3}, & \dots r_{1,n} \\ 0, & \mu_2, & r_{2,3}, & \dots r_{2,n} \\ 0, & 0, & \mu_3, & \dots r_{3,n} \\ \dots & \dots & \dots & \dots \\ 0, & 0, & 0, & \dots \mu_n \end{array} \right\|$$

One of the minors of this matrix is $r_{1,2} \times \mu_3 \dots \times \mu_n$, which cannot be divisible by ∇_{n-1} or $\mu_2 \times \mu_3 \times \dots \times \mu_n$, unless $r_{1,2}$ is a multiple of μ_2 ; but $r_{1,2} < \mu_2$, because $\|\nabla_{n-1}\|$ is reduced, therefore $r_{1,2}=0$. Similarly, it may successively be shown that $r_{1,3}=0 \dots r_{1,n}=0$. Now if the matrix

$$\left\| \begin{array}{cccc} \mu_2, & r_{2,3}, & \dots r_{2,n} \\ 0, & \mu_3, & \dots r_{3,n} \\ \dots & \dots & \dots \\ 0, & 0, & \dots \mu_n \end{array} \right\| \quad \dots \quad (77.)$$

which is of the type $(n-1) \times (n-1)$, be reduced to the form

$$\|v'\| \times \left\| \frac{\nabla_{n-1}}{\nabla_{n-2}}, \frac{\nabla_{n-2}}{\nabla_{n-3}}, \dots \frac{\nabla_1}{\nabla_0} \right\| \times \|u'\|,$$

in which $\nabla_{n-2}, \nabla_{n-3}, \dots$ represent the greatest common divisors of the minors of (77.), we may replace $\|\nabla_{n-1}\|$ by the matrix

$$\|\nabla_{n-1}\| = \begin{vmatrix} 1 & 0 \\ 0 & v' \end{vmatrix} \times \left\| 1, \frac{\nabla_{n-1}}{\nabla_{n-2}}, \frac{\nabla_{n-2}}{\nabla_{n-3}}, \dots, \frac{\nabla_1}{\nabla_0} \right\| \times \begin{vmatrix} 1 & 0 \\ 0 & u' \end{vmatrix},$$

where $\begin{vmatrix} 1 & 0 \\ 0 & v' \end{vmatrix}$ and $\begin{vmatrix} 1 & 0 \\ 0 & u' \end{vmatrix}$ denote unit-matrices of the type $n \times n$, the forms of which are sufficiently indicated by the symbols themselves. Hence, observing that

$$\begin{bmatrix} 1 & 0 \\ 0 & u' \end{bmatrix} \times \left\| \frac{\nabla_n}{\nabla_{n-1}}, 1, 1, \dots \right\| = \left\| \frac{\nabla_n}{\nabla_{n-1}}, 1, 1, \dots \right\| \times \begin{bmatrix} 1 & 0 \\ 0 & u' \end{bmatrix},$$

and that

$$\left\| 1, \frac{\nabla_{n-1}}{\nabla_{n-2}}, \frac{\nabla_{n-2}}{\nabla_{n-3}}, \dots, \frac{\nabla_1}{\nabla_0} \right\| \times \left\| \frac{\nabla_n}{\nabla_{n-1}}, 1, 1, \dots \right\| = \left\| \frac{\nabla_n}{\nabla_{n-1}}, \frac{\nabla_{n-1}}{\nabla_{n-2}}, \dots, \frac{\nabla_1}{\nabla_0} \right\|,$$

we obtain, from (76.),

$$\|x\| = \|v\| \times \left\| \begin{pmatrix} 1 & 0 \\ 0 & v' \end{pmatrix} \right\| \times \left\| \begin{pmatrix} \nabla_n & \nabla_{n-1} & \dots & \nabla_1 \\ \nabla_{n-1} & \nabla_{n-2} & \dots & \nabla_0 \end{pmatrix} \right\| \times \left\| \begin{pmatrix} 1 & 0 \\ 0 & u' \end{pmatrix} \right\| \times \|w^{-1}\|,$$

or more simply,

$$\|a\| = \|\alpha\| \times \left\| \frac{\nabla_n}{\nabla_{n-1}}, \frac{\nabla_{n-1}}{\nabla_{n-2}}, \dots, \frac{\nabla_1}{\nabla_0} \right\| \times \|\beta\|.$$

It has, however, still to be shown that $\nabla_{n-2}, \nabla_{n-3}, \dots$ which have been defined with reference to the matrix (77.) are the greatest common divisors of the successive systems of minors of $\|a\|$. These greatest common divisors are the same for the given matrix $\|a\|$ and for the matrix $\left\| \frac{\nabla_n}{\nabla_{n-1}}, \frac{\nabla_{n-1}}{\nabla_{n-2}}, \dots, \frac{\nabla_1}{\nabla_0} \right\|$ which is derived from it by multiplication with unit-matrices; consequently ∇_{n-1} divides every first minor of $\left\| \frac{\nabla_n}{\nabla_{n-1}}, \frac{\nabla_{n-1}}{\nabla_{n-2}}, \dots, \frac{\nabla_1}{\nabla_0} \right\|$, and, in particular, it divides $\frac{\nabla_n}{\nabla_{n-1}} \times \frac{\nabla_{n-2}}{\nabla_{n-3}} \times \frac{\nabla_{n-3}}{\nabla_{n-4}} \times \dots \times \frac{\nabla_1}{\nabla_0} = \frac{\nabla_n \times \nabla_{n-2}}{\nabla_{n-1}}$; *i. e.* $\frac{\nabla_{n-1}}{\nabla_{n-2}}$ divides $\frac{\nabla_n}{\nabla_{n-1}}$. Again, $\nabla_{n-1}, \nabla_{n-2}, \dots, \nabla_1, \nabla_0$, which are the determinant and greatest common divisors of the minors of (77.), are also the determinant and greatest common divisors of the minors of the matrix

[illegible]

so that if $s \leq n-2$, ∇_s divides every minor of order s in (78.), and, consequently, the minor $\frac{\nabla_{s+1}}{\nabla_s} \times \frac{\nabla_{s-1}}{\nabla_{s-2}} \times \frac{\nabla_{s-2}}{\nabla_{s-3}} \times \dots \times \frac{\nabla_1}{\nabla_3}$; or $\frac{\nabla_s}{\nabla_{s-1}}$ divides $\frac{\nabla_{s+1}}{\nabla_s}$. It thus appears that in the series of numbers

$$\frac{\nabla n}{\nabla n-1}, \frac{\nabla n-1}{\nabla n-2}, \dots, \frac{\nabla 2}{\nabla 1}, \frac{\nabla 1}{\nabla 0}$$

each term is divisible by that which comes after it. Every product of s terms of that series is therefore divisible by the product $\frac{\nabla_s}{\nabla_{s-1}} \times \frac{\nabla_{s-1}}{\nabla_{s-2}} \times \dots \times \frac{\nabla_1}{\nabla_0} = \nabla_s$; or, which is the same thing, ∇_s is the greatest common divisor of the minors of order s in the reduced matrix (78.), and therefore in the given matrix $\|a\|$.

Art. 15. If the proposed matrix $\|a\|$ be not square, but of the type $n \times (n+m)$, let $\|a\| = \|\nabla_n\| \times \|a'\|$, where $\|a'\|$ is a prime matrix of the same type as $\|a\|$, and $\|\nabla_n\|$ a square matrix, of which the determinant is ∇_n , the greatest divisor of $\|a\|$. Then if $\|\nabla_n\|$ be expressed in the form

$$\|v\| \times \left\| \frac{\nabla_n}{\nabla_{n-1}}, \frac{\nabla_{n-1}}{\nabla_{n-2}}, \dots, \frac{\nabla_1}{\nabla_0} \right\| \times \|u\|,$$

and if, for brevity, we write $\|V\|$ for $\|u\| \times \|a'\|$, we obtain for $\|a\|$ the expression

$$\|a\| = \|v\| \times \left\| \frac{\nabla_n}{\nabla_{n-1}}, \frac{\nabla_{n-1}}{\nabla_{n-2}}, \dots, \frac{\nabla_1}{\nabla_0} \right\| \times \|V\|. \quad (79.)$$

The numbers $\nabla_n, \nabla_{n-1}, \dots$, which are the greatest common divisors of the minors of $\|\nabla_n\|$, are also by the theorem of art. 12, the greatest common divisors of the minors of $\|a\|$. We see therefore that $\frac{\nabla_s}{\nabla_{s-1}}$ is always divisible by $\frac{\nabla_{s-1}}{\nabla_{s-2}}$, in the case of an oblong as well as a square matrix.

Art. 16. To show still more clearly the nature of the quotients $\frac{\nabla_s}{\nabla_{s-1}}$, we add the following proposition:—

“If in any rectangular matrix we divide each minor determinant of order s by the greatest common divisor of its own first minors, the greatest common divisor of all the quotients thus obtained is $\frac{\nabla_s}{\nabla_{s-1}}$.”

By this proposition $\frac{\nabla_s}{\nabla_{s-1}}$ is itself defined as a greatest common divisor, instead of being defined as the quotient of one greatest common divisor, divided by another.

To establish its truth we may first consider the quotient $\frac{\nabla_n}{\nabla_{n-1}}$ in any rectangular matrix $\|A\|$ of the type $n \times (m+n)$. Let ω denote the greatest common divisor of the quotients obtained by dividing each determinant of $\|A\|$ by the greatest common divisor of the first minors of that determinant: we have then to show that

$$\frac{\nabla_n}{\nabla_{n-1}} = \omega.$$

Since the greatest common divisor of any vertical column of minors in $\|A\|$ is not altered by premultiplication with a unit-matrix, it is evident that ω as well as $\frac{\nabla_n}{\nabla_{n-1}}$ will remain unchanged by that operation. If, therefore,

$$\|A\| = \|v\| \times \left\| \frac{\nabla_n}{\nabla_{n-1}}, \frac{\nabla_{n-1}}{\nabla_{n-2}}, \dots, \frac{\nabla_1}{\nabla_0} \right\| \times \|V\|, \quad (79.)$$

where $\|v\|$ is a unit, and $\|V\|$ a prime matrix, we may consider instead of $\|A\|$, the simpler matrix

$$\left\| \frac{\nabla_n}{\nabla_{n-1}}, \frac{\nabla_{n-1}}{\nabla_{n-2}}, \dots, \frac{\nabla_1}{\nabla_0} \right\| \times \|V\|. \quad (80.)$$

Let $\|\theta_1\|, \|\theta_2\|, \dots$ &c. be the different square matrices of $\|V\|$; $\theta_1, \theta_2, \dots$ their determi-

nants; ψ_i the greatest common divisor of those first minors in $\|\theta_i\|$ which do not contain the constituents of its uppermost row, so that $\frac{\theta_i}{\psi_i}$ is integral; lastly, let ω_i be the quotient obtained by dividing the determinant

$$\left\| \frac{\nabla_n}{\nabla_{n-1}}, \frac{\nabla_{n-1}}{\nabla_{n-2}}, \dots, \frac{\nabla_1}{\nabla_0} \right\| \times \|\theta_i\|, \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (81.)$$

by the greatest common divisor of its first minors, so that ω is the greatest common divisor of $\omega_1, \omega_2, \dots$. Now the greatest common divisor of the first minors of (81.) is evidently divisible by ∇_{n-1} , and divides $\nabla_{n-1} \times \psi_i$ (because $\nabla_{n-1} \psi_i$ is the greatest common divisor of one of its rows of minors). Consequently ω_i divides $\nabla_n \theta_i \div \nabla_{n-1}$, and is divisible by $\nabla_n \theta_i \div \nabla_{n-1} \psi_i$. Therefore $\frac{\nabla_n}{\nabla_{n-1}}$ is a common divisor of certain numbers respectively dividing the numbers $\omega_1, \omega_2, \dots$, viz. the numbers $\frac{\nabla_n}{\nabla_{n-1}} \cdot \frac{\theta_i}{\psi_i}$; it is also (because $\theta_1, \theta_2, \dots$ are relatively prime) the greatest common divisor of the numbers $\frac{\nabla_n}{\nabla_{n-1}} \theta_i$, in which the same numbers ω_i are respectively contained; *i. e.* $\frac{\nabla_n}{\nabla_{n-1}}$ is the greatest common divisor of the numbers $\omega_1, \omega_2, \dots$ themselves, or

$$\frac{\nabla_n}{\nabla_{n-1}} = \omega.$$

By the aid of this particular case of the theorem the general proposition itself may be proved as follows:—

If in any rectangular matrix of the type $n \times (m+n)$ we propose to determine Ω_s , the greatest common divisor of the quotients obtained by dividing each minor determinant of order s , by the greatest common divisor of its own first minors, we may begin by selecting any s vertical columns [$s < n$], and forming the proper quotient for each determinant of order s , contained in this partial matrix of the type $n \times s$. Let λ_i denote the greatest common divisor of these quotients; then, as we have just seen, λ_i is the greatest common divisor of all the determinants of the partial matrix, divided by the greatest common divisor of all its first minors. Hence (by art. 12) λ_i will remain unchanged when the given matrix is premultiplied by a unit-matrix. But Ω_s is the greatest common divisor of all the divisors $\lambda_1, \lambda_2 \dots$ corresponding to every group of s vertical columns; therefore Ω_s is itself unchanged by premultiplication. Similarly, if a *square* matrix be post-multiplied by a rectangular prime matrix, it may be shown that Ω_s is the same for the given square matrix, and for the resulting rectangular matrix. Hence if, as before,

$$\|A\| = \|v\| \times \left\| \frac{\nabla_n}{\nabla_{n-1}}, \dots, \frac{\nabla_1}{\nabla_0} \right\| \times \|V\|,$$

Ω_s and $\frac{\nabla s}{\nabla_{s-1}}$ are the same for $\left\| \frac{\nabla n}{\nabla_{n-1}}, \frac{\nabla_{n-1}}{\nabla_{n-2}}, \dots \frac{\nabla_1}{\nabla_0} \right\|$ and for $\|A\|$. But in the matrix $\left\| \frac{\nabla n}{\nabla_{n-1}}, \dots \frac{\nabla_1}{\nabla_0} \right\|$ it is evident that $\frac{\nabla s}{\nabla_{s-1}}$ and Ω_s coincide; therefore in any rectangular matrix

$$\frac{\nabla_s}{\nabla_{s-1}} = \Omega_s.$$

From the definition of $\frac{\nabla_s}{\nabla_{s-1}}$ as a greatest common divisor, which we have now obtained, we infer that if $\|D\|$ be any matrix containing another matrix $\|\nabla\|$, and if $D_s, D_{s-1} \dots \nabla_s, \nabla_{s-1}, \dots$ be the greatest common divisors of the corresponding minors in $\|D\|$ and $\|\nabla\|$ respectively, not only is ∇_s divisible by D_s , and ∇_{s-1} by D_{s-1} , but also $\frac{\nabla_s}{\nabla_{s-1}}$ by $\frac{D_s}{D_{s-1}}$.

It is not difficult to show that in any matrix $\frac{\nabla_s}{\nabla_{s-k}}$ is the greatest common divisor of all the quotients obtained by dividing each minor of order s by the greatest common divisor of its minors of order $s-k$. But as this extension of the preceding result is not needed in what follows, we may omit it here.

We may add, that the theorem of this article is precisely equivalent to the following, which may be demonstrated by a different method.

“If P^I be the highest power of a given prime that divides all the minors of order s in a given matrix, and if all the minors of order $s-1$ contained in one particular minor of order s are divisible by P^{I-s+1} , that minor is itself divisible by P^{I+s} .”

It should be observed that whenever all the minors of any determinant are zero, the quotient obtained by dividing the determinant by the greatest common divisor of its minors is also zero.

Art. 17. These results admit of immediate application to the theory of systems of linear congruences. The general type of such systems is

$$\left. \begin{aligned} A_{i,1}x_1 + A_{i,2}x_2 + \dots + A_{i,n}x_n &\equiv A_{i,n+1}, \text{ mod. } M \\ i &= 1, 2, 3, \dots n' \end{aligned} \right\}; \dots \dots \dots (82.)$$

and to construct a complete theory of them it is requisite, first, to assign a criterion for their resolvability or irresolvability; secondly, when they are resolvable, to investigate the number of incongruous solutions of which they are susceptible; and, lastly, to exhibit a method for obtaining all these solutions. We shall first suppose that $n'=n$; i. e. that the proposed system is neither defective nor redundant.

Let $D_n, D_{n-1} \dots \nabla_n, \nabla_{n-1}, \dots$ respectively denote the greatest common divisors of the determinants and minors of the augmented and unaugmented matrices of the system (82.); also let $\delta_n, \delta_{n-1}, \dots \delta_1$ denote the greatest common divisors of M with $\frac{\nabla_n}{\nabla_{n-1}}$, of M with $\frac{\nabla_{n-1}}{\nabla_{n-2}}, \dots$, and let $d_n, d_{n-1} \dots$ similarly represent the greatest common divisors of M with $\frac{D_n}{D_{n-1}}$, of M with $\frac{D_{n-1}}{D_{n-2}}, \&c.$; then, if $d = d_n \times d_{n-1} \times \dots \times d_1$, $\delta = \delta_n \times \delta_{n-1} \times \dots \times \delta_1$, we have the two following theorems:

(i.) “The necessary and sufficient condition for the resolvability of the system (81.) is $d = \delta$.”

(ii.) “When this condition is satisfied, the number of its incongruous solutions is d .”

To demonstrate the first of these theorems, we revert to the principle of art. 11, from which it appears that the necessary and sufficient condition for the resolvability of the system (82.) is that the greatest divisors of the two matrices

$$\left\| \begin{array}{c} M, 0, 0, \dots, 0, A_{1,1}, \dots, A_{1,n} \\ 0, M, 0, \dots, 0, A_{2,1}, \dots, A_{2,n} \\ 0, 0, M, \dots, 0, A_{3,1}, \dots, A_{3,n} \\ \dots \\ 0, 0, 0, \dots, M, A_{n,1}, \dots, A_{n,n} \end{array} \right\| \dots \dots \dots (83.)$$

and

$$\left\| \begin{array}{c} M, 0, 0, \dots, 0, A_{1,1}, \dots, A_{1,n+1} \\ 0, M, 0, \dots, 0, A_{2,1}, \dots, A_{2,n+1} \\ 0, 0, M, \dots, 0, A_{3,1}, \dots, A_{3,n+1} \\ \dots \\ 0, 0, 0, \dots, M, A_{n,1}, \dots, A_{n,n+1} \end{array} \right\| \dots \dots \dots (84.)$$

are to be equal to one another. Now the first of those greatest common divisors is evidently the greatest common divisor of

$$M^n, M^{n-1} \nabla_1, M^{n-2} \nabla_2, \dots, M \nabla_{n-1}, \nabla_n;$$

which, for brevity, we shall represent by the symbol

$$[M^n, M^{n-1} \nabla_1, M^{n-2} \nabla_2, \dots, \nabla_{n-1} M, \nabla_n]. \dots \dots \dots (85.)$$

Let $M = P \times Q \times R \dots$, P, Q, R, \dots denoting powers of different primes; we may then, in (85.), replace M by P, Q, R, \dots successively, since

$$\begin{aligned} & [M^n, M^{n-1} \nabla_1, \dots, M \nabla_{n-1}, \nabla_n] \\ &= [P^n, P^{n-1} \nabla_1, \dots, P \nabla_{n-1}, \nabla_n] \times [Q^n, Q^{n-1} \nabla, \dots, \nabla_n] \times \dots \end{aligned}$$

If P divide any one of the numbers $\frac{\nabla_s}{\nabla_{s-1}}, \dots$, let $\frac{\nabla_s}{\nabla_{s-1}}$ be the least of them that it divides;

also let $P_i = \left[P, \frac{\nabla_i}{\nabla_{i-1}} \right]$; so that $P_i = P$, if $i \geq s$. Then

$$\begin{aligned} & [P^n, P^{n-1} \nabla_1, \dots, P \nabla_{n-1}, \nabla_n] \\ &= P_1 \times \left[\frac{P^n}{P_1}, P^{n-1} \frac{\nabla_1}{P_1}, P^{n-2} \frac{\nabla_2}{P_1}, \dots, \frac{\nabla_n}{P_1} \right] \\ &= P_1 \times \left[P^{n-1}, P^{n-2} \frac{\nabla_2}{\nabla_1}, P^{n-3} \frac{\nabla_3}{\nabla_1}, \dots, \frac{\nabla_n}{\nabla_1} \right], \end{aligned}$$

observing that $\frac{\nabla_1}{P_1}$ is prime to P [if $s > 1$], and that we may therefore divide the last n numbers by $\frac{\nabla_1}{P_1}$; and may then omit $\frac{P^n}{P_1}$, which is divisible by P^{n-1} . Continuing this process, we find

$$\begin{aligned} & [P^n, P^{n-1} \nabla_1, \dots, P \nabla_{n-1}, \nabla_n] \\ &= P_1 \times P_2 \times \dots \times P_{s-1} \left[P^{n-s+1}, P^{n-s} \frac{\nabla_s}{\nabla_{s-1}}, P^{n-s-1} \frac{\nabla_{s+1}}{\nabla_{s-1}}, \dots, \frac{\nabla_n}{\nabla_{s-1}} \right]; \end{aligned}$$

or, since $\frac{\nabla_s}{\nabla_{s-1}}$ is divisible by P , and $\frac{\nabla_{s+k}}{\nabla_{s-1}} = \frac{\nabla_{s+k}}{\nabla_{s+k-1}} \times \frac{\nabla_{s+k-1}}{\nabla_{s+k-2}} \dots \times \frac{\nabla_s}{\nabla_{s-1}}$ by P^{k+1} ,

$$\begin{aligned} & [P^n, P^{n-1} \nabla_1, P^{n-2} \nabla_2, \dots, P \nabla_{n-1}, \nabla_n] \\ &= P_1 \times P_2 \times P_3 \dots \times P_{s-1} \times P^{n-s+1} \\ &= \prod_{i=1}^n P_i. \end{aligned}$$

But $\delta_i = P_i \times Q_i \times R_i \times \dots$; and consequently the greatest common divisor of the determinants of (83.) is $\delta_1 \times \delta_2 \times \dots \times \delta_n$ or δ . Similarly, the greatest divisor of (84.) is $d_1 \times d_2 \times \dots \times d_n$ or d . The necessary and sufficient condition for the resolvability of the proposed system of congruences is therefore contained in the formula

$$d = \delta.$$

It should, however, be observed that, since $\frac{D_s}{D_{s-1}}$ divides $\frac{\nabla_s}{\nabla_{s-1}}$ (art. 16), d_s divides δ_s , and therefore the equation

$$d = \delta$$

involves the coexistence of the n equations

$$d_1 = \delta_1, d_2 = \delta_2, \dots, d_n = \delta_n. \quad (86.)$$

To investigate the number of solutions of the system (82.), supposed to be resolvable, let $\|\alpha\|$ and $\|\beta\|$ be two unit-matrices satisfying the equation

$$\|\alpha\| \times \|A\| \times \|\beta\| = \left\| \frac{\nabla_n}{\nabla_{n-1}}, \frac{\nabla_{n-1}}{\nabla_{n-2}}, \dots, \frac{\nabla_1}{\nabla_0} \right\|; \quad (87.)$$

also let

$$\begin{aligned} x_i &= \beta_{i,1} v_1 + \beta_{i,2} v_2 + \dots + \beta_{i,n} v_n \\ i &= 1, 2, 3, \dots, n \\ c_i &= \alpha_{i,1} A_{1,n+1} + \alpha_{i,2} A_{2,n+1} + \dots + \alpha_{i,n} A_{n,n+1} \\ i &= 1, 2, 3, \dots, n. \end{aligned}$$

Then it is evident that the proposed system of congruences is precisely equivalent to the system

$$\left. \begin{aligned} \frac{\nabla_{n-i+1}}{\nabla_{n-i}} v_i &\equiv c_i, \text{ mod. } M, \\ i &= 1, 2, 3, \dots, n \end{aligned} \right\} \quad (88.)$$

in such a manner that the two systems are simultaneously resolvable or irresolvable; and that from any number of incongruous solutions of the one an equal number of incongruous solutions of the other is deducible. But the whole number of incongruous solutions of (88.) is $\delta_1 \times \delta_2 \times \dots \times \delta_n = \delta$; *i. e.* the number of solutions of the proposed system is δ .

By the use of the unit-matrices $\|\alpha\|$ and $\|\beta\|$ the actual resolution of the proposed system is made to depend on the resolution of the n congruences contained in (88.). But this method of solving a system of linear congruences, though very symmetrical, is perhaps too tedious for the purposes of computation.

Art. 18*. Let the proposed system of congruences be the *defective* system

$$\left. \begin{aligned} A_{i,1}x_1 + A_{i,2}x_2 + \dots + A_{i,n+m}x_{n+m} &\equiv A_{i,n+m+1}, \text{ mod. } M, \\ i &= 1, 2, 3, \dots, n, \end{aligned} \right\} \dots \dots \dots (89.)$$

and let the notation of the last Article be retained. It is easily seen that the condition of resolvibility of the system (89.) is, as before,

$$\delta = d.$$

But the number of its incongruous solutions, when that condition is satisfied, is not δ , but $\delta \times M^m$. For we have seen that we can find a unit-matrix $\|a\|$, and a prime matrix $\|A'\|$ of the type $n \times (n+m)$, satisfying the equation

$$\|a\| \times \|A\| = \left\| \frac{\nabla_n}{\nabla_{n-1}}, \frac{\nabla_{n-1}}{\nabla_{n-2}}, \dots, \frac{\nabla_2}{\nabla_1}, \frac{\nabla_1}{\nabla_0} \right\| \times \|A'\|;$$

we may therefore replace the system (89.) by a system of the form

$$\frac{\nabla_{n-i+1}}{\nabla_{n-i}} U_i \equiv C_i, \text{ mod. } M, \dots \dots \dots (90.)$$

in which

$$U_i = A'_{i,1}x_1 + A'_{i,2}x_2 + \dots + A'_{i,n+m}x_{n+m},$$

and

$$C_i = \alpha_{i,1} A_{1,n+m+1} + \alpha_{i,2} A_{2,n+m+1} + \dots + \alpha_{i,n} A_{n,n+m+1}.$$

If the system (89.) is resolvable, the system (90.) will be so too, and will give d or δ different systems of values for U_1, U_2, \dots, U_n , any one of which may be represented by the formula

$$\left. \begin{aligned} U_i &\equiv u_i, \text{ mod. } M, \\ i &= 1, 2, 3, \dots, n \end{aligned} \right\} \dots \dots \dots (91.)$$

Let us replace the modulus M by P , the highest power of one of its prime divisors. Since $\|A'\|$ is a prime matrix, one at least of its determinants, for example, the determinant $\Sigma \pm A'_{1,1} A'_{2,2} \dots A'_{n,n}$, is prime to P . It will follow from this that, whatever values we attribute to $x_{n+1}, x_{n+2}, \dots, x_{n+m}$, each of the δ systems represented by (91.) is resolvable for the modulus P , and gives, for any assumed values of $x_{n+1}, x_{n+2}, \dots, x_{n+m}$, only one set of values of x_1, x_2, \dots, x_n . Each of those δ systems admits, therefore, of P^m solutions for the modulus P , *i. e.* of M^m for the modulus M . The system (89.) will consequently admit of $\delta \times M^m$ solutions.

Let us also consider the *redundant* system of congruences,

$$\left. \begin{aligned} A_{i,1}x_1 + A_{i,2}x_2 + \dots + A_{i,n}x_n &\equiv A_{i,n+1}, \text{ mod. } M, \\ i &= 1, 2, 3, \dots, n+m, \end{aligned} \right\} \dots \dots \dots (92.)$$

and let D_{n+1} denote the greatest divisor of its augmented matrix. Let p represent a prime divisor of M , and let $p^\theta, p^{I_s}, p^{I_s}$ be the highest powers of p , which divide M, D_s, ∇_s respectively. The condition of resolvibility of art. 11, applied to the system (92.), considered with respect to the modulus p^θ , becomes, after division by $p^{(m-1)\theta}$,

$$\left. \begin{aligned} [p^{I_{n+1}}, p^{I_n+\theta}, p^{I_{n-1}+2\theta}, \dots, p^{(n+1)\theta}] \\ = [p^{I_n+\theta}, p^{I_{n-1}+2\theta}, \dots, p^{(n+1)\theta}] \end{aligned} \right\} \dots \dots \dots (93.)$$

* [This article has been added since the paper was read. The theorems contained in it are supplementary to that of the preceding article. September 1861, H. J. S. S.]

And this equation is impossible, if $\theta > I_{n+1} - I_n$. For $I_{s+1} - I_s \geq I_s - I_{s-1}$, because $\frac{D_{s+1}}{D_s}$ is divisible by $\frac{D_s}{D_{s-1}}$; the inequality, $I_{n+1} < I_n + \theta$, involves, therefore, the inequalities

$$\left. \begin{array}{l} I_{n+1} < I_{n-s+1} + s\theta, \\ s=1, 2, 3, \dots n+1, \end{array} \right\} \dots \dots \dots (94.)$$

and these, again, imply the corresponding inequalities

$$\left. \begin{array}{l} I_{n+1} < i_{n-s+1} + s\theta, \\ s=1, 2, 3, \dots n+1, \end{array} \right\} \dots \dots \dots (95.)$$

because $I_{n-s+1} \leq i_{n-s+1}$. From (94.) it appears that the value of $[p^{I_{n+1}}, p^{I_n+\theta}, \dots p^{(n+1)\theta}]$ is $p^{I_{n+1}}$, and from (95.), that the value of $[p^{i_{n+1}}, p^{i_{n-1}+2\theta}, \dots p^{(n+1)\theta}]$ is a power of p superior to $p^{I_{n+1}}$; *i. e.* the equation (93.) is impossible. We thus obtain, as a first condition for the resolubility of the proposed system (92.), the congruence

$$\frac{D_{n+1}}{D_n} \equiv 0, \text{ mod. M. } \dots \dots \dots (96.)$$

When this condition is satisfied, we obtain from (93.), omitting the term $p^{I_{n+1}}$ (because $I_n + \theta \geq I_n + \theta$), and dividing by p^θ , the equation of condition,

$$\begin{aligned} & [p^{I_n}, p^{I_{n-1}+\theta}, p^{I_{n-2}+2\theta}, \dots p^{n\theta}] \\ & = [p^{i_n}, p^{i_{n-1}+\theta}, p^{i_{n-2}+2\theta}, \dots p^{n\theta}], \end{aligned}$$

which leads us (as in the last article) to the simple formula

$$d = \delta.$$

This equation, therefore, and the congruence (96.), express the necessary and sufficient conditions for the resolubility of the proposed redundant system.

When these two conditions are simultaneously satisfied, the number of incongruous solutions is δ . For, if we again consider the proposed system of congruences with respect to the modulus p^θ , and select from it a partial system of n congruences such that the determinants of its augmented matrix, which are necessarily divisible by p^{I_n} , are not divisible by any higher power of p , it is readily seen that every set of values of the indeterminates $x_1, x_2, \dots x_n$, which satisfies the partial system, will also (by virtue of the inequality $\theta \leq I_{n+1} - I_n$) satisfy the remaining congruences of the proposed system. The number of solutions of the proposed system is therefore the same as that of the partial system. And because p^{I_n} the highest power of p which divides every determinant of order n in the augmented matrix of the proposed system is also the highest power of p which divides the augmented matrix of the partial system, it follows from the last theorem of art. 16, that $p^{I_{n-1}}, p^{I_{n-2}}, \dots$ are the highest powers of p which divide the corresponding orders of determinants in the latter, as well as in the former matrix. The number of solutions of the partial system (and consequently of the proposed system), considered with respect to the modulus p^θ , is therefore expressed by the formula

$$[p^{I_n}, p^{I_{n-1}+\theta}, \dots p^{n\theta}];$$

or, finally, the number of solutions of the proposed system, considered with respect to M as modulus, is d or δ .

Art. 19. We shall terminate this paper with an elementary theorem relating to linear systems of equations, which admits of frequent application in other parts of the theory of numbers.

Resuming the notation of art. 11, we may see from the theorem of that article, that if the system (56.) be resolvable for any given values of the numbers $A_{1,0}, A_{2,0}, \dots A_{n,0}$, it is also resolvable for any other values of those numbers, respectively congruous, for the modulus D , to the given values; so that the resolvability or irresolvability of the system depends exclusively on the residues of the numbers $A_{i,0}$, mod. D . There are D^n possible combinations of these residues, and we shall now show that for D^{n-1} of them the system is resolvable, while for the remaining $D^{n-1} (D-1)$ it is irresolvable. For this purpose let

$$\|\alpha\| \times \|A\| = \left\| \frac{D_n}{D_{n-1}}, \frac{D_{n-1}}{D_{n-2}}, \dots \frac{D_1}{D_0} \right\| \times \|A'\|, \quad . \quad . \quad . \quad . \quad . \quad (97.)$$

$\|\alpha\|$ denoting a unit-matrix, and $\|A'\|$ a prime matrix of the same type as $\|A\|$, while D_n, D_{n-1}, D_1, D_0 are of course the greatest common divisors of the determinants and minors of $\|A\|$. Let also

$$-C_i = A_{1,0} \alpha_{i,1} + A_{2,0} \alpha_{i,2} + \dots + A_{n,0} \alpha_{i,n}.$$

The given system is then exactly equivalent to the system

$$\left. \begin{aligned} \frac{D_{n-i+1}}{D_{n-i}} [A'_{i,1} x_1 + A'_{i,2} x_2 + \dots + A'_{i,n+m} x_{n+m}] &= C_i \\ i &= 1, 2, 3, \dots n. \end{aligned} \right\} \quad . \quad . \quad . \quad . \quad . \quad (98.)$$

For the resolvability of this system it is requisite that C_i should be divisible by $\frac{D_{n-i+1}}{D_{n-i}}$; and this condition is sufficient as well as necessary, because $\|A'\|$ is a prime matrix. Now of the D or D_n values, incongruous for the modulus D , which may be attributed to C_i , $\frac{D_n \times D_{n-i}}{D_{n-i+1}}$ are divisible by $\frac{D_{n-i+1}}{D_{n-i}}$; whence it is evident that of the D^n systems of values which may be attributed to $C_1, C_2, \dots C_n$, $D^n \div \left[\frac{D_1}{D_0} \cdot \frac{D_2}{D_1} \cdot \frac{D_3}{D_2} \dots \frac{D_n}{D_{n-1}} \right]$, *i. e.* D^{n-1} render the system (98.) resolvable. Consequently the given system is also resolvable for D^{n-1} , and no more, of the systems of values that can be attributed (mod. D) to $A_{1,0}, A_{2,0}, \dots A_{n,0}$.

Art. 20. The methods employed in the present paper are without exception such as to be immediately applicable to any species of complex numbers which admit of resolution into actual or ideal prime factors. And the greater part of the results at which we have arrived may be transferred, *mutatis mutandis*, to the theories of such numbers. For example, if in the equations (56.) we suppose the constituents of $\|A\|$ to represent complex numbers, it will be found that the criterion for the resolvability or irresolvability of the system, which we have demonstrated in the case of ordinary integers, applies equally in the case of complex numbers; and again, the condition of resolvability of a system of congruences of which the modulus as well as the coefficients are complex numbers, is

